⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　平4－163768

| ⑤Int. Cl.³ | 識別記号 | 庁内整理番号 | ④公開　平成4年(1992)6月9日 |
|---|---|---|---|
| G 11 B 20/12 | | 9074－5D | |
| 20/00 | Z | 9197－5D | |

審査請求　未請求　請求項の数 4　（全7頁）

⑤発明の名称　ディスク機密保護方式および装置

⑳特　願　平2－288528
㉒出　願　平2(1990)10月29日

㉗発 明 者　大 山　光 男　東京都国分寺市東恋ケ窪1丁目280番地　株式会社日立製作所中央研究所内
㉗発 明 者　荒 澤　伸 幸　東京都国分寺市東恋ケ窪1丁目280番地　株式会社日立製作所中央研究所内
㉘出 願 人　株式会社日立製作所　東京都千代田区神田駿河台4丁目6番地
㉙代 理 人　弁理士 小川 勝男　外1名

明　細　書

1．発明の名称

ディスク機密保護方式および装置

2．特許請求の範囲

1．ディスク記憶媒体上に、ファイルを記憶するファイル記憶部と、ファイル記憶部へのファイルの記憶を管理制御する管理情報を記憶するための管理情報記憶部とを有してなるディスク記憶媒体において、ファイル記憶部に記憶するデータを、データ変換鍵により一意的に定まるデータ変換手順によりデータ変換したデータとし、管理情報記憶部に記憶される管理情報を、少なくとも、ファイルを識別するためのファイル名と、ファイルの長さと、ファイルのロケーションと、該データ変換鍵とを含んで構成し、かつ管理記憶部に記録する該管理情報を暗号化して記録することを特徴とするディスク機密保護方式。

2．カートリッジ内にディスク記憶媒体と、半導体メモリを具備して成り、ディスク記憶媒体上にファイルを記憶し、ディスク記憶媒体へのファイルの記憶を管理制御するための管理情報を該半導体メモリに記憶するディスクカートリッジにおいて、ディスク記憶媒体に記憶するデータを、データ変換鍵により一意的に定まるデータ変換手順によりデータ変換したデータとし、該半導体メモリに記憶するファイル管理情報は、少なくとも、ファイルを識別するためのファイル名、ファイルの長さ、ファイルのロケーション、該データ変換鍵を含んで構成し、かつ該半導体メモリに記録する該管理情報を暗号化して記録することを特徴とするディスク機密保護方式。

3．請求項1記載のディスク記憶媒体が装着され、該ディスク記憶媒体にファイルをリードノライトするディスク記憶装置において、暗号化鍵の入力手段と、復号鍵の入力手段と、データ変換鍵の入力手段と、該データ変換鍵をファイル管理情報の構成要素として登録する手段と、該データ変換鍵により一意的に定まるデータ変換手

段によりデータ変換を行う手段と、データ変換されてディスク記憶媒体に記憶されたデータを、該データ変換鍵を用いて復元する手段と、ファイル管理情報を、入力された該暗号化鍵を用いて暗号化し、管理情報記録部に書き込む手段と、管理情報記録部に暗号化して記録されている管理情報を読みだし、入力された該復号鍵を用いて暗号を解読し、平文に変換する手段とを備えたことを特徴とするディスク記憶装置。

4．請求項2記載のディスクカートリッジが装着され、該ディスクカートリッジにファイルをリード／ライトするディスク記憶装置において、暗号化鍵の入力手段と、復号鍵の入力手段と、データ変換鍵の入力手段と、該データ変換鍵をファイル管理情報の構成要素として登録する手段と、ディスク記憶媒体に記憶するデータを該データ変換鍵により一意的に定まるデータ変換手順によりデータ変換する手段と、データ変換されてディスク記憶媒体に記憶されたデータを、該データ変換鍵を用いて復元する手段と、管理情報を、入力された該暗号化鍵を用いて暗号化し、ディスクカートリッジに内蔵される半導体メモリに書き込む手段と、該半導体メモリから暗号化して記録された管理情報を読みだし、入力された該復号鍵を用いて暗号を解読し、平文に変換する手段とを備えたことを特徴とするディスク記憶装置。

3．発明の詳細な説明

〔産業上の利用分野〕

本発明は、特に着脱可能な記憶媒体、例えばフロッピディスク，光ディスク等に好適な機密保護方式および装置に関する。

〔従来の技術〕

近年、重要なデータが多量にコンピュータシステムに蓄積されるようになり、重要情報，機密情報の漏洩，改竄が大きな問題になってきている。このような状況にあって、機密保護の簡便な方式としてパスワードが用いられてきた。すなわち、ＯＳ（オペレーティングシステム）の管理のもとにパスワードを登録しておき、ユーザは、システムを利用する際パスワードを入力し、ＯＳは登録されているパスワードとユーザが入力したパスワードを比較し、一致すればシステムの利用を許可するようにしていた。しかし、この方法では、記憶装置に着脱可能な記憶媒体、たとえばフロッピディスクや光ディスクでは、記憶媒体自身では機密保護機能を持たないので、他のシステムでは第三者がアクセスでき、機密保護はなされない。

これを防ぐため、特開平1－158724 号公報で開示されている方式では、記憶媒体からファイル読みだす際に、ファイルに付加されているパスワードと、ユーザが入力したパスワードを照合し、一致したときのみファイルの読みだしを許可するようにしている。また、特開平1－309120 号公報で開示されている方式では、記憶媒体にパスワードをマウントしておき、記憶媒体イニシャライズの際、入力されたパスワードと記憶媒体にマウントされたパスワードを照合し、一致したときのみイニシャライズを実行している。

〔発明が解決しようとする課題〕

特開平1－158724号公報，特開平1－309120号公報で開示されている方式では、パスワードを照合する機能を備えた記憶装置に装着して使用されるかぎり、パスワードを知らない者のファイル読みだし、あるいは、記憶媒体のイニシャライズを防ぐことができる。しかし、記憶装置に着脱可能な記憶媒体、例えばフロッピディスク、光ディスクなどでは、記憶媒体を装着する記憶装置がパスワードの照合機能を持っていないか、あるいは、故意にパスワードの照合を省略した場合は、ファイルの内容を容易に読みだし、あるいはイニシャライズすることができる。すなわち、記憶媒体自体は機密保護機能を持っておらず、十分な機密保護ができない場合がある。

本発明の目的は、記憶媒体自体に機密保護機能を付加し、第三者が容易にアクセス出来ないようにして、機密保護機能を強化することにある。

〔課題を解決するための手段〕

上記目的を達成するために、本発明では、

(1) 記憶媒体上に、少なくとも、ファイル名，フ

ファイルのサイズ，ロケーション，データ変換鍵を含んで構成されるファイル管理情報を暗号化して登録し，

(2) 記憶媒体にファイルを記憶する際、データ変換鍵により一意的に定まるデータ変換手順によってデータ変換して記録するようにした．

さらに、本発明では、上記方式を実現するための記憶装置を提供する．すなわち、着脱可能なフロッピディスク，光ディスク等を記憶媒体とするディスク記憶装置において、暗号化回路，復号回路，暗号化鍵入力手段，復号鍵入力手段，データ変換鍵入力手段，データ変換／データ復元回路を設けた．そして、記憶媒体上のファイル管理情報を暗号化して記録するようにした．

〔作用〕

ユーザは，記憶媒体にアクセスする際，暗号化鍵，復号鍵を入力し，新たにファイルを書き込む場合にはさらにデータ変換鍵を入力する．そして、本発明による記憶装置は，記憶媒体にファイル管理情報を書き込む場合、入力された暗号化鍵と暗号化回路を用いて暗文に変換して書き込む．逆に、ファイル管理情報を読みだす場合は，復号鍵と復号回路により、暗文から平文に変換する．

これにより、暗号化鍵と復号鍵を知らない者はファイル管理情報にアクセスすることが出来ないので、結局、記憶媒体上のファイルを正しくアクセスすることが困難になり、機密が保たれる，また、記憶媒体上のファイル管理情報が暗号化されることにより、記憶媒体自体で機密保護が可能になる．

さらに本発明では，記憶媒体にファイルを記憶する際，データ変換鍵を用いて、データ変換回路によりデータ変換して書き込み、逆に記憶媒体からファイルを読みだす際は、データ変換鍵を用いて、データ復元回路により復元して読みだす．これにより、たとえ特殊な手段により記憶媒体上のデータを直接読みだすことができた場合にも、データ変換鍵を知らなければ，正確に復元することは困難であり，機密が保護される．

また，データ変換鍵は，ファイル管理情報の構成要素として，暗号化して記憶媒体上に記憶されるので，復号鍵を知らないとデータ変換鍵を正しく読みだすことはできない．

〔実施例〕

本発明の第1の実施例によるディスク記憶装置の構成を第1図に、第1図に示す装置の動作を説明するフローチャートを第7図に示し、以下に説明する．

第1図において，20はフロッピディスク，光ディスク等の着脱可能なディスク，14はディスク記憶媒体，15はディスク記憶媒体上のファイル管理情報格納領域，1はディスク記憶装置に装着されたディスク20にデータをリード／ライトするホストコンピュータ，2はディスク記憶装置にホストコンピュータ1を接続するためのインタフェース，3はディスク記憶装置を制御するためのマイクロプロセッサ，4はマイクロプロセッサ3で実行する制御プログラムが格納されるROM，5はマイクロプロセッサ3のワーク領域として機能するRAM，6はスピンドルモータ16，アクチュエータ機構17，リードライト回路18を制御するための制御インタフェース，7はファイル管理領域15に書き込むデータを、暗号化鍵レジスタ9に保持される暗号化鍵を用いて暗号化するための暗号化回路，8はファイル管理領域15から読みだす暗号化されたデータを、復号鍵レジスタ10に保持される復号鍵を用いて解読し、平文に変換するための復号回路，12は速度調整用バッファメモリ，13は暗号化されていない（平文の）ファイル管理情報を格納するためのメモリ，25はデータ変換鍵レジスタ26に保持されるデータ変換鍵を用いて、ディスク記憶媒体14に記憶するファイルをデータ変換して記憶し，逆にディスク記憶媒体から読みだしたデータを復元するためのデータ変換／データ復元回路である．

第5図にデータ変換／復元回路の一構成例を示す．第5図において，記憶媒体に記憶されるデータ101はN個の排他的論理和回路30－1，30－Nによりビット反転され変換データ102となり、逆に記憶媒体から読みだされた変換デー

タ102はN個の排他的論理和31-1，31-Nにより再度ビット反転されてもとのデータ101に復元される。このとき、反転されるビットの数と位置はデータ変換鍵のビットパターンにより定まる。したがって、例えばデータ変換鍵の長さは64ビット以上あれば選択可能なビットパターンの数は膨大になり、データ変換鍵のビットパターンを知らないかぎりデータの復元は極めて困難になる。

次に、第7図に示すフローチャートを用いて第1図に示すディスク記憶装置の動作を説明する。最初にアクセス対象のディスク20をディスク記憶装置に装着し、ホストコンピュータ1よりディスク記憶装置を起動する。ユーザは、暗号化鍵、復号鍵を入力し、新たにファイルを書き込む場合は、さらにデータ変換鍵を入力する700。入力された暗号化鍵、復号鍵は、インタフェース2，コマンド線101，プロセッサインタフェース11を介して、マイクロプロセッサ3により暗号化鍵レジスタ9、復号鍵レジスタ10にセットされる。マイクロプロセッサ3は、ディスク記憶媒体14上のファイル管理領域15から暗号化されたファイル管理情報を読みだし、復号鍵を用いて復号回路8により暗号を解読して平文に変換し、ファイル管理情報の写し格納メモリ13に格納する701。ホストコンピュータからリード/ライト要求を受けると、マイクロプロセッサ3は、ファイル管理情報の写し格納メモリ13からファイル管理情報を読み取り、アクセスすべきファイルの属性、サイズ、ロケーション、データ変換鍵等の情報を得、データ変換鍵をデータ変換鍵レジスタ26にセットする702。

次に、マイクロプロセッサ3は、読み取ったファイル管理情報をもとに、ホストコンピュータ1との間でインタフェース2を介して、リード/ライトデータのやりとりを行い、ライトの場合は、データ変換/データ復元回路25，リード/ライト回路18を介して変換データをディスク記憶媒体14に書き込む。一方、リードの場合はリード/ライト回路18を介してディスク記憶媒体14から読みだした変換データ102をデータ変換/復元回路25により復元して101、ホストコンピュータ1に読みだす703。次に、ディスクへのリード/ライトを行った結果、ファイル管理情報の更新が必要かどうかを調べる604。そして、更新が必要であれば、ファイル管理情報の写し格納メモリ13の内容を更新するとともに、暗号化鍵を用いて暗号化回路7により更新内容を暗号化してディスク記憶媒体14上のファイル管理領域15の内容を更新する。そしてこのとき、ファイルの新たな書き込みがあった場合は、そのとき使用したデータ変換鍵をファイル管理情報として登録し、暗号化してディスク記憶媒体14に記憶する705。

以上に説明したディスク記憶装置の制御は、制御プログラムとして記述され、ROM4に格納されており、マイクロプロセッサ3で実行することにより実現される。

このように、ファイル管理情報を暗号化しておくことにより、暗号化鍵、復号鍵を持つ者以外はファイル管理情報を読むことができないので、所望のファイルのサイズ，ロケーション，属性等がわからず、ディスク記憶媒体へのリード/ライトを正しく行うことが困難になり、機密が保護される。

また、データ変換鍵がファイル管理情報の構成要素としてディスク記憶媒体14に記憶されるので、新たにファイルを書き込む場合以外はデータ変換鍵を入力する必要がなく、かつデータ変換鍵は暗号化して記憶されるので、ディスク記憶媒体からファイル管理情報を読みだせた場合にも、データ変換鍵を解読することは困難であり、機密が保護される。

以上、本発明の第1の実施例では、ファイル管理情報がディスク記憶媒体14上に記録される場合について説明した。しかし、ファイル管理情報がディスク記憶媒体14上に記録されると、ファイル管理情報を更新する毎にディスク記憶媒体14上のファイル管理領域15にアクセスすることが必要になり、ディスクのリード/ライトのス

ループットが低下する。これを避けるため、第4図に示すように、ディスクカートリッジ21に高速半導体メモリ22を埋め込み、この半導体メモリ22にファイル管理情報を格納する方式がある。この場合、この半導体メモリ22に格納するファイル管理情報を暗号化し、ディスク記憶媒体14に、データ変換を施した変換データを記憶することにより、ディスクカートリッジ21自体で機密保護を行うことができる。

第6図は、本発明の第2の実施例によるディスク記憶装置の構成を示す図、第8図はその動作を説明するフローチャートである。第6図において、21はディスクカートリッジであり、第4図に示すように、データを記録するディスク記憶媒体14とは別に、カートリッジに埋め込まれた半導体メモリ22を有しており、暗号化したファイル管理情報が格納される。23は外部から半導体メモリ22にアクセスするためのコネクタである。

第6図に示すディスク記憶装置において、暗号化されたファイル管理情報の入出力が、コネクタ23を介してカートリッジに埋め込まれた半導体メモリ22に対して行われること、およびファイル管理情報の写し格納領域が必要に応じてRAM5上に設けられること以外は第1図に示すディスク記憶装置に同じである。半導体メモリのアクセス時間は、ディスクのアクセス時間に比べて一般に十分短い。したがって、復号回路8による暗号の解読が十分速く実行できれば、半導体メモリ22に格納されている管理情報の写しをRAM5上に持つ必要はなく、直接半導体メモリ22をアクセスすればよい。

なお、以上の説明では、暗号化鍵と復号鍵が異なる、公開鍵暗号による暗号化を行う場合について説明したが、秘密鍵暗号による暗号化を行う場合は、暗号化鍵と復号鍵は共通であるので、暗号化鍵レジスタ9と復号鍵レジスタ10は共通にできる。

〔発明の効果〕

以上に説明したように、本発明によればディスクカートリッジ、あるいはディスク記憶媒体自体が機密保護機能を持つので、パスワードを付加する方式に比べ、特に着脱可能なディスク記憶媒体において、機密保護機能が強化されるという効果がある。

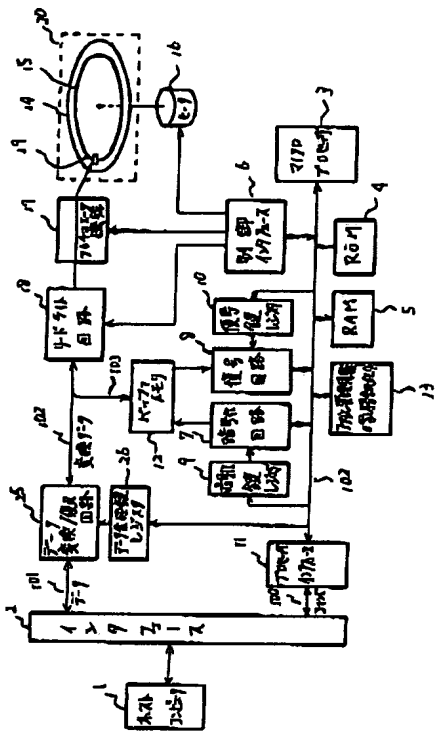
4．図面の簡単な説明

第1図は第1の実施例によるディスク記憶装置の構成を示す図、第2図は本発明の方式を説明する図、第3図はファイル管理情報の構成例を示す図、第4図は半導体メモリを有するディスクカートリッジを示す図、第5図はデータ変換／復元回路の一構成例を示す図、第6図は第2の実施例によるディスク記憶装置の構成を示す図、第7図は第1図に示す装置の動作を説明するフローチャート図、第8図は第6図に示す装置の動作を説明するフローチャート図である。

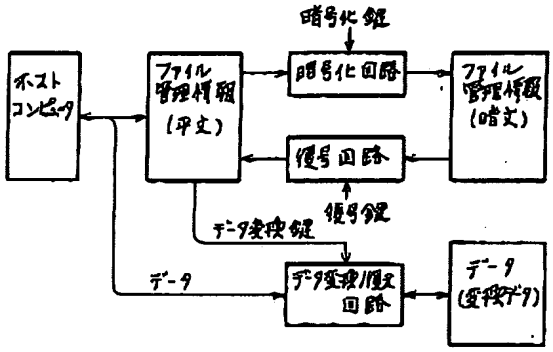
1…ホストコンピュータ、3…マイクロプロセッサ、4…ROM、5…RAM、7…暗号化回路、8…復号回路、9…暗号化鍵レジスタ、10…復号鍵レジスタ、12…バッファメモリ、13…ファイル管理情報の写し格納メモリ、20…ディスク、21…半導体メモリを有するディスクカートリッジ、22…半導体メモリ、23…コネクタ、25…データ変換鍵レジスタ、26…データ変換／復元回路。

代理人　弁理士　小川勝男

第 1 図



第 2 図

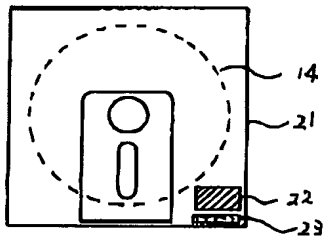



第 3 図

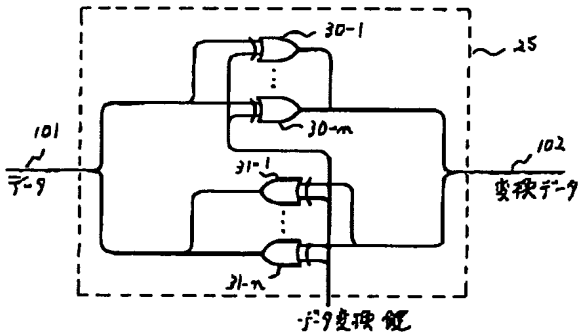
ファイル管理情報の一構成例

| | | | | |
|---|---|---|---|---|
| ファイル名 #1 | 属性 #1 | サイズ #1 | ロケーション #1 | データ変換鍵 #1 |
| ファイル名 #2 | 属性 #2 | サイズ #2 | ロケーション #2 | データ変換鍵 #2 |
| ファイル名 #n | 属性 #n | サイズ #n | ロケーション #n | データ変換鍵 #n |

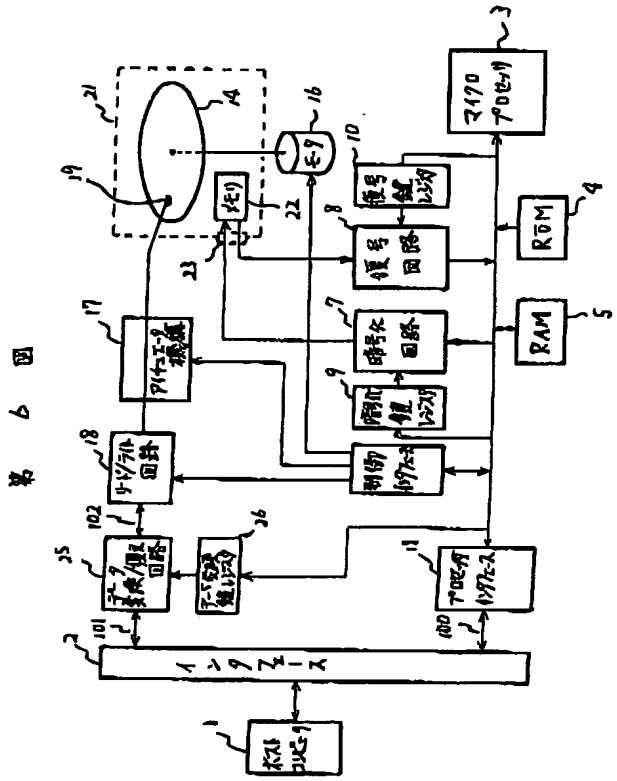
第 4 図



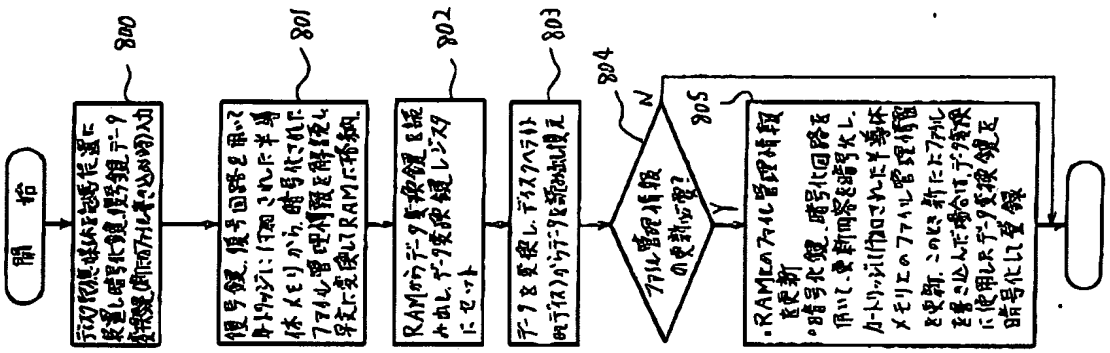
第 5 図




第 6 図



第8図




第7図